



Securing The Enterprise

Tony Rybczynski, Nortel Network

Nortel Network Security Solutions for Enterprises

Nortel Networks Security Solutions are based on a tested, reliable architecture that accelerates the performance of traditional technologies to provide high-performance security services. Nortel Networks full portfolio of Security Solutions provide integrated firewall functionality and management capabilities, scalability and ease-of-provisioning, and the top-rated security consulting team in the industry. Specifically, our Security Solutions allow enterprises to provide the mission-critical applications and selective Internet access employees need to succeed while simultaneously protecting the enterprises' investments from external hazards such as viruses and hackers. Enterprises can offer protected, controlled connectivity to telecommuters, branch sites, partners and customers -- but keep out unwanted visitors so their networks and web sites can run safely and securely. Nortel Networks security portfolio includes Shasta Broadband Service Nodes, Contivity VPN switches, Alteon iSD-SSL Accelerators, Alteon Web Switches and Preside RADIUS servers. In addition, Nortel Networks security professionals provides a range of security services including: vulnerability scans, firewall configuration service, and liability training. Finally, Nortel Networks Optical Ethernet solutions create new opportunities for service providers in the delivery of managed security services.

Broadly speaking, there are two environments in which enterprises operate: the enterprise network and the Internet. The enterprise network connects enterprise sites together, is tuned for performance, is designed for reliability, and traditionally is a closed system with relatively high security. This is the back-office network that provides connectivity to data warehouses, applications, and human resources across the corporation. These sites are interconnected via

physical and virtual circuits, and most recently via Optical Ethernet connectivity. On the other hand, the Internet is all about access to the Web at large, and ubiquitous reach via IP VPNs to customers, remote and mobile employees, partners, and increasingly remote sites. The marriage of the Internet and wireless systems is even extending its reach beyond the wired world. It's all about low-cost connectivity on demand, and turning an inherently open environment into a secure business tool.

Protecting enterprise assets across these two environments is a major challenge for IT organizations, complicated by the many potential electronic points of entry to enterprise resources. There are hopefully a limited number of formal high-speed gateways between the Internet and the enterprise. However, there are other points of entry that need to be included in an overall security strategy. For example, telecommuters who stay connected via DSL or cable modems need to be protected because their always-on Internet access provides an opportunity for any hacker who gains access to the PC to gain access to enterprise resources piggybacking on or emulating an authenticated user. Rogue wireless LAN users within the enterprise can also pose a threat whenever they are within range of a wireless base station (e.g., from public areas within or outside of an office building). Even visitors plugging into a DHCP-enabled LAN jack in a conference room can present a security threat.

A comprehensive approach to network security starts with a threat assessment and the establishment of an overall security policy across the enterprise. Such a policy has to recognize that, according to the FBI's Computer Security Institute, 48 percent of all attacks originate from within the enterprise. Building total security into every application is expensive, and doesn't address the need to protect the enterprise

network itself. Therefore, network-based security that restricts the flow of information to and from the enterprise network, is shared across applications, and off-loads the application has become a common practice. Network-based security does not obviate the need for application level mechanisms like those required to protect the integrity of user information.

THE FIREWALL

A fundamental network-based functional building block that provides network access controls at the boundaries between the hostile Internet and the enterprise and within the enterprise itself is what is generally called a firewall. This access control can be applied to employees, partners, or other outside users trying to gain access to certain applications (servers) or networks within an organization's infrastructure. Authorization is the process by which a decision is made to grant or deny a request for access, typically based on the authenticated identity of the requester. This concept is often expressed as a question, such as "Can this user do what they are asking to do?" depending on whether the request is to access information, modify information, or take a specific action. The term "firewall" derives from the barrier that was installed between a car engine (the Internet is the engine of growth) and the passengers (the critical assets in any enterprise) to protect them from fires and explosions (hackers and other infiltrators).

What's A Firewall?

A firewall is a network security device that protects a private network from unauthorized access -- much like the way that a security guard controls access to a building by examining the credentials of individuals attempting to enter. A firewall makes these decisions based on the corporate security policy, to which the firewall has been configured. Firewalls can also be deployed internally to protect a sensitive section of a corporate network from unauthorized users. With a sensible security policy and an up-to-date security rule set designed to implement that policy, a firewall can protect an enterprise network from a broad range of attacks.

What Do Firewalls Do?

A firewall filters both inbound and outbound traffic. It can also manage access to networked resources, such as host applications. It can be used to log all attempts to enter the private

network and trigger alarms when hostile or unauthorized entry is attempted. There are two access denial methodologies used by firewalls. A firewall may allow all traffic through unless it meets certain criteria, or it may deny all traffic unless it meets certain criteria. The type of criteria used depends on the network layer at which the criteria are being applied. Static packet filtering is generally done at the IP layer though deep packet filtering can go into higher layer headers (e.g. port number). TCP proxies operate at the session layer, while stateful inspection operates with an understanding of the application.

STATIC FILTERING BY THE PACKET

The first, and most basic, line of defense in firewall protection is packet filtering. Packet filters examine incoming and outgoing packets and apply a fixed set of rules to the packets to determine whether they will be allowed to pass. Depending on the packet and the criteria, the firewall can drop the packet, forward it, or send a message to the originator. Rules can include source and destination IP addresses, source and destination port numbers, and protocol used. The advantage of packet filtering is the low cost and low impact on network performance. For example, it is easy to filter out all packets destined for port 80, which might normally be the port for a Web server. The administrator may decide that port 80 is off-limits except for specific IP addresses, and a packet filter would suffice for this.

A malicious hacker may try to gain entry by "spoofing" the source IP address of packets sent to the firewall. An effective measure against IP spoofing is the use of a virtual private network (VPN) protocol such as IPSec. This methodology involves encryption of the data in the packet as well as the source address. The VPN software or firmware decrypts the packet and the source address and performs a checksum. If either the data or the source address has been tampered with, the packet will be dropped. Without access to the encryption keys, a potential intruder would be unable to penetrate the firewall.

TCP PROXIES

TCP is the most common protocol used directly above the IP level. A TCP proxy monitors TCP handshaking to determine whether a requested TCP session is legitimate. It can check IDs and

passwords for a TCP session request and implement proxy connection authorization or other authentication services. Information passed to a remote computer through a TCP gateway appears to have originated from the gateway. This generally means that a client outside the firewall cannot see or directly connect to a machine protected by the firewall. A TCP proxy has the advantage of hiding information about the private network from the Internet user.

TCP proxies are often integrated with user authentication schemes including mechanisms such as RADIUS (literally, Remote Authentication for Dial-In User Service but also covering Dedicated Internet User Services), SecureID, and Public Key Infrastructure (PKI). For example, a RADIUS server authenticates every user requesting access from the Internet, grants each user the appropriate level of service, and tracks their usage of network resources.

STATEFUL PACKET INSPECTION

Stateful packet inspection provides the highest level of security without any compromise to network performance. Stateful inspection extracts the state-related information required for security decisions from all application layers and maintains this information in dynamic-state tables for evaluating subsequent connections attempts. Stateful inspection examines the transaction conditions between the client and the application or between two interoperating applications, and knows what is “normal.”

Stateful inspection is the opposite of packet filtering or TCP proxies, by being application specific rather than general purpose. It can determine whether session packets are legitimate and evaluate contents of packets at the application layer. It can run application specific proxies, or rely on stateful algorithms to recognize and process application layer data. For example, stateful inspection can examine packets at the application layer, can filter application specific commands such as FTP Put and Get commands, and be used to log user application logins and activity. This cannot be accomplished by packet filtering or TCP proxies, since these do not know anything about the application level. By definition, stateful inspection is not transparent to end-users and requires configuration of each client computer. Stateful packet inspection provides a solution that is

highly secure and offers maximum performance, scalability and extensibility.

IMPLEMENTING FIREWALLS

Security is a business-critical activity, which needs to be addressed through a well-defined security policy. Different firewall technologies are an important element of the technological arsenal, and are a key function of what some call the Intelligent Internet. These need to be deployed wherever the Internet touches: at central sites, at remote offices, and in standalone PCs.

Firewalls are offered either as a software application or packaged as part of a hardware solution. Given the growth of VPNs, extranet switches are key network building blocks that combine packet filtering, TCP proxies and stateful inspection, with IP VPN termination to provide security to the network and protection of data from unauthorized external intrusion. Extranet switches handle up to 100 protocols, including FTP, Telnet, H323, RealAudio, across multiple physical and logical ports, achieving peak performance through advanced memory management techniques and optimized packet inspection. These can support half a million concurrent sessions, establish tens of thousands of sessions per second, while statefully inspecting hundreds of Mbps of data. Advanced features include protection from denial of service attacks, Syn floods, and spoofing.

While firewalls have been traditionally implemented internally by using standalone firewall products or extranet switches, there is a growing trend to turn to Internet and Security Service Providers, and system integrators. This recognizes that while critical security controls such as definitions of authenticated users and firewall rule sets must remain within the enterprise, the implementation and management of firewalls may be handled more effectively by organizations that specialize in security controls, and can maintain the required breadth of knowledgeable resources. Outsourcing requires a highly reliable, high bandwidth and low latency network connection (e.g. based on Optical Ethernet) be established between the enterprise network and the outsourcer's facility.



Tony Rybczynski is Director of Strategic Marketing and Technologies in Nortel Networks Enterprise Optical Ethernet Solutions. He has over 29 years experience in the application of packet network technology. He writes a monthly 'Inside Networking' column in Communications Solutions magazine.

Reprinted from *Communications Solutions*® magazine, volume 2, dated January 2002, published by Technology Marketing Corporation, One Technology Plaza, Norwalk, CT 06854 USA. Copyright © 2000 Technology Marketing Corporation, all rights reserved. For information about annual subscriptions, call 800-243-6002 or 203-852-6800 or visit the publication's Web site at www.tmcnet.com.

For more information:

<http://www.nortelnetworks.com/opticalethernet>

Nortel, Nortel Networks, the Nortel Networks corporate logo, the globemark design, Contivity, Alteon, Shasta and Preside are trademarks of Nortel Networks.